Coding Rules

Coding Rules are not stored, organized, or displayed like other articles in the Build Security In site. They are isolated into a separate area of the site in order to make searching and browsing them easier. Searches performed from this page will only span Coding Rules, not other articles. To view other BSI articles, click here[1] or click **Home** in the navigation menu to the left.

Description

Coding rules are representations of knowledge, gained from real-world experiences, about potential vulnerabilities that exist in programming languages like C and C++. As we create and use software with a given coding environment, we discover and learn about many vulnerabilities that exist in this environment, how to recognize whether they crop up in our code, and what to do to fix them. Coding Rules are the codification of this knowledge.

This catalog provides a set of Coding Rules to assist software developers, whether manually or in conjunction with tools, to discover, explore, remove and eventually prevent security vulnerabilities in their code.

The content, schema, categorization and coverage of the Coding Rules is fairly complex. It is strongly recommended that you read the Coding Rules Overview document before diving into the Coding Rules themselves.

Overview Articles

Name	Version Creation Time	Abstract
Coding Rules Overview	5/16/08 2:38:36 PM	Coding rules are representations of knowledge, gained from real-world experiences, about potential vulnerabilities that exist in programming languages like C and C++. As we create and use software with a given coding environment, we discover and learn about many vulnerabilities that exist in this environment, how to recognize whether they crop up in our code, and what to do to fix them.

Browse Rules by Facets

[2]

Most Recently Updated Rules [Ordered by Last Modified Date]

Name	Version Creation Time	Abstract
Wsprintf	5/16/08 2:39:40 PM	Be careful with string formatting operations.
UnicodeToBytes	5/16/08 2:39:39 PM	Poses a risk of buffer overflow if the return buffer is not appropriately sized.
Unlink	5/16/08 2:39:39 PM	Vulnerable to TOCTOU issues
Utime	5/16/08 2:39:39 PM	Vulnerable to TOCTOU issues
Utmpname	5/16/08 2:39:39 PM	Vulnerable to TOCTOU issues

All Rules [Ordered by Title]

Name	Version Creation Time	Abstract
A2W-Macro	5/16/08 2:39:13 PM	Long strings can overflow stack
access()	5/16/08 2:39:13 PM	Never use simply to avoid changing to a less privileged mode
acct()	5/16/08 2:39:13 PM	Be careful with location specified, especially use of NULL
AddAccess-ACE	5/16/08 2:39:13 PM	Access Control Entries not inheritable
AfxLoadLibrary	5/16/08 2:39:14 PM	Vulnerable to "tainted" DLLs placed in a location in the search path before the intended DLL
AfxParseURL	5/16/08 2:39:14 PM	Does not fully comply with URL standards
au_to_path()	5/16/08 2:39:14 PM	Be careful with paths passed as a parameter
basename()	5/16/08 2:39:14 PM	Vulnerable to path spoofing

2. https://buildsecurityin.us-cert.gov/daisy/bsi-rules/facetedBrowser/coding-rules

bcopy()	5/16/08 2:39:14 PM	Be careful with buffer size and termination
bind()	5/16/08 2:39:14 PM	Race and conflict conditions with mulitple processes or threads attempting to bind to the same port and IP adress
BytesToUnicode	5/16/08 2:39:14 PM	Be careful with size parameters
CanShareFolderW	5/16/08 2:39:15 PM	Be careful of malicious folder substitution
Catgets	5/16/08 2:39:15 PM	Be careful of function use of environment variables for search path
Catopen	5/16/08 2:39:15 PM	Be careful of function's implicit use of environment variables
CHMOD	5/16/08 2:39:15 PM	Vulnerable to TOCTOU issues
CHOWN	5/16/08 2:39:15 PM	Vulnerable to TOCTOU issues
CHROOT-01	5/16/08 2:39:15 PM	Unset root SUID after calling chroot()
CHROOT-02	5/16/08 2:39:15 PM	Call chdir("/") after using the chroot()
CHROOT-03	5/16/08 2:39:16 PM	Close file descriptors when using chroot()
CHString(Format)	5/16/08 2:39:16 PM	Be careful with string formatting operations
CIN	5/16/08 2:39:17 PM	>> operator does not perform bounds checking
Copylist()	5/16/08 2:39:17 PM	Vulnerable to TOCTOU issues
CREAT	5/16/08 2:39:17 PM	Potential for unintentional file deletion and unstable race conditions
CreateFile-01	5/16/08 2:39:17 PM	Always use CREATE_NEW
CreateFile-02	5/16/08 2:39:17 PM	Don't rely on HIDDEN, INDEXED, and ARCHIVE for file security
CreateProcess-01	5/16/08 2:39:17 PM	Close process and thread handles after calling CreateProcess()
CreateProcess-02	5/16/08 2:39:17 PM	Parent process has explicit trust from child
CreateProcess-03	5/16/08 2:39:18 PM	Use restrictive permissions when creating a new process
CreateProcess-04	5/16/08 2:39:18 PM	Fully qualify executable filename
CreateThread	5/16/08 2:39:18 PM	Use restrictive permissions when creating new threads

CreateUrlCacheEntry	5/16/08 2:39:18 PM	Return value buffer must be large enough to store returned path
CRYPT-01	5/16/08 2:39:18 PM	crypt() is cryptographically weak; use stronger alternatives
CRYPT-02	5/16/08 2:39:18 PM	To hide passwords, always use with a random salt for each hash
CString(Format)	5/16/08 2:39:18 PM	Be careful with string formatting operations
CUSERID	5/16/08 2:39:19 PM	Never rely on username for security - (Function is obsolete)
Database Functions	5/16/08 2:39:19 PM	Vulnerable to TOCTOU issues
DIRNAME	5/16/08 2:39:19 PM	Vulnerable to TOCTOU issues
Dlopen()	5/16/08 2:39:19 PM	Vulnerable to TOCTOU issues
EnterCriticalSection	5/16/08 2:39:19 PM	Thread termination or critical section deletion can cause undefined state
Exec	5/16/08 2:39:20 PM	Vulnerable to TOCTOU issues
Exec-SearchPath-01	5/16/08 2:39:20 PM	Path-searching Exec functions are susceptible to malicious programs inserted into the search path
Exec-SearchPath-02	5/16/08 2:39:20 PM	Non-pathsearching Exec functions that run both .com and .exe files can be fooled into running malicious programs
Executable-Icon-Location	5/16/08 2:39:20 PM	Carefully manage destination buffer size
File Streams	5/16/08 2:39:20 PM	Vulnerable to TOCTOU issues
FindExecutableImage	5/16/08 2:39:21 PM	Return value buffer must be large enough to hold returned path
FormatMessage	5/16/08 2:39:21 PM	Vulnerable to string formatting issues
FREOPEN	5/16/08 2:39:21 PM	Vulnerable to TOCTOU issues
Ftw and Nftw	5/16/08 2:39:21 PM	Vulnerable to TOCTOU issues
GetAttr	5/16/08 2:39:21 PM	Remember to free memory if numerous calls made
GETC	5/16/08 2:39:21 PM	Be careful of buffer sizes and null termination when using getc()
GetEnv	5/16/08 2:39:22 PM	Be careful of buffer length when using returned value
GetExtensionVersion	5/16/08 2:39:22 PM	Executes with elevated privileges. Use only for intended purposes.
GetFileNameFromBrowse	5/16/08 2:39:22 PM	Return buffer length should be MAX_PATH length

GetFullPathName	5/16/08 2:39:22 PM	Carefully manage buffer sizes
GETHOST	5/16/08 2:39:22 PM	Make deep copies of static return data before issuing a new API call
GETLOGIN	5/16/08 2:39:23 PM	Results of getlogin() should not be trusted
GetLongPathName	5/16/08 2:39:23 PM	Carefully manage buffer sizes
GETOPT	5/16/08 2:39:23 PM	Vulnerable to internal buffer overflows
GETPASS	5/16/08 2:39:24 PM	Vulnerable to internal buffer overflows
GETS	5/16/08 2:39:24 PM	Function is intrinsically unsafe and should not be used
GetTempFileName	5/16/08 2:39:24 PM	Use randomly generated prefix value to ensure filename that is more difficult to guess
GETTEMPPATH	5/16/08 2:39:24 PM	Vulnerable to several path and buffer issues
GETTEXT	5/16/08 2:39:24 PM	Susceptible to environment variable driven buffer overflows
GETWD	5/16/08 2:39:24 PM	Carefully manage buffer sizes (getwd() is deprecated)
InitializeCriticalSection	5/16/08 2:39:24 PM	Unsafe low memory exceptions on some platforms. Always delete critical section before reinitializaing.
Kerberos	5/16/08 2:39:25 PM	Functions vulnerable to TOCTOU issues
Kerberos	5/16/08 2:39:25 PM	Functions vulnerable to TOCTOU issues
Kvm_open	5/16/08 2:39:25 PM	Be very careful with privilege mode of calling process
Link	5/16/08 2:39:25 PM	Vulnerable to TOCTOU issues
LoadLibrary	5/16/08 2:39:25 PM	Use fully-qualified filename to ensure that LoadLibrary() will load the correct library
LoadModule	5/16/08 2:39:26 PM	Use fully-qualified path/filename to ensure that LoadModule() will load the correct file (LoadModule() is deprecated)
MALLOC-OVERFLOW	5/16/08 2:39:26 PM	An integer overflow can cause malloc() to allocate less memory than required
Mbstowcs	5/16/08 2:39:26 PM	Ensure output buffer size is properly specified and large enough

MEMCOPY	5/16/08 2:39:26 PM	Carefully manage size of destination buffer
MEMSET	5/16/08 2:39:26 PM	Using memset to scrub sensitive data in memory does not usually work unless the data is used subsequently.
MetaRule	5/16/08 2:39:26 PM	Buffer Management
MetaRule	5/16/08 2:39:26 PM	Impersonation - Carefully check for call failure to avoid unintended privilege escalation
MetaRule	5/16/08 2:39:26 PM	Multibyte Chars
MetaRule	5/16/08 2:39:26 PM	Path Management
MetaRule	5/16/08 2:39:27 PM	Random
MetaRule	5/16/08 2:39:27 PM	String Formatting
MKDIR	5/16/08 2:39:27 PM	Vulnerable to TOCTOU issues
MKFIFO	5/16/08 2:39:27 PM	Vulnerable to TOCTOU issues
MKNOD	5/16/08 2:39:27 PM	Vulnerable to TOCTOU issues
Mkstemp	5/16/08 2:39:27 PM	Don't be complacent. Several vulnerabilities possible.
MKTEMP	5/16/08 2:39:27 PM	Temp file name easy to guess. Vulnerable to TOCTOU. (Function should not be used)
Mount()	5/16/08 2:39:27 PM	Vulnerable to TOCTOU issues
MoveFile	5/16/08 2:39:28 PM	Indeterminate whether expected ACL exists on file after move (function is deprecated)
Nlist	5/16/08 2:39:28 PM	Vulnerable to TOCTOU issues
OemToChar	5/16/08 2:39:28 PM	Carefully manage unit sizes and buffer bounds checking
OPEN	5/16/08 2:39:28 PM	Vulnerable to TOCTOU issues
OPENDIR	5/16/08 2:39:28 PM	Vulnerable to TOCTOU issues
PathAddBackslash	5/16/08 2:39:29 PM	Return value buffer must be large enough to store returned path
PathAddExtension	5/16/08 2:39:29 PM	Return value buffer must be large enough to store returned path
PathAppend	5/16/08 2:39:29 PM	The output buffer must be sized to hold at least MAX_PATH characters
PathBuildRoot	5/16/08 2:39:29 PM	The output buffer must be large enough to hold four characters
PathCanonicalize	5/16/08 2:39:29 PM	The destination string buffer must be long enough to hold the return file path

PathCleanupSpec	5/16/08 2:39:29 PM	The destination string buffer must be long enough to hold the return file path
PathCombine	5/16/08 2:39:29 PM	The output buffer must be sized to hold at least MAX_PATH characters
PathCommonPrefix	5/16/08 2:39:29 PM	The destination string buffer must be long enough to hold the return file path
PATHCONF	5/16/08 2:39:30 PM	Vulnerable to TOCTOU issues
PathFindOnPath	5/16/08 2:39:30 PM	The destination string buffer must be long enough to hold the return file path
PathGetShortPath	5/16/08 2:39:30 PM	The destination string buffer must be long enough to hold the return file path
PathMakeUniqueName	5/16/08 2:39:30 PM	Generated pathname easily guessed
PathQuoteSpaces	5/16/08 2:39:30 PM	The destination string buffer must be long enough to hold the return file path
PathRelativePathTo	5/16/08 2:39:30 PM	The destination string buffer must be long enough to hold the return file path
PathRenameExtension	5/16/08 2:39:30 PM	The destination string buffer must be long enough to hold the return file path
PathResolve	5/16/08 2:39:30 PM	The destination string buffer must be long enough to hold the return file path
QuerySecurityContextToken	5/16/08 2:39:31 PM	A failure of the QuerySecurityContextToken must be detected and handled
Readlink	5/16/08 2:39:31 PM	Value written in the output buffer is not null-terminated and may not contain the entire file name
Readlink	5/16/08 2:39:31 PM	Vulnerable to TOCTOU issues
READ-OVERFLOW	5/16/08 2:39:31 PM	Must ensure that the buffer is large enough to hold the number of bytes read
REALLOC	5/16/08 2:39:31 PM	Not suitable for use with secure memory because memory contents are not zeroed out
REALPATH	5/16/08 2:39:31 PM	The destination string buffer must be long enough to hold the return file path. Never use this function

		(or do so at very high potential risk).
RecvMsg	5/16/08 2:39:31 PM	Carefully manage buffer size and ensure remote host is validated
REMOVE	5/16/08 2:39:32 PM	Vulnerable to TOCTOU issues
RENAME	5/16/08 2:39:32 PM	Vulnerable to TOCTOU issues
RMDIR	5/16/08 2:39:32 PM	Vulnerable to TOCTOU issues
SCANDIR	5/16/08 2:39:32 PM	Vulnerable to TOCTOU issues
SCANF	5/16/08 2:39:33 PM	Very susceptible to buffer overflow
Select	5/16/08 2:39:33 PM	Requires close bounds checking
SetEntriesInAcl	5/16/08 2:39:33 PM	Problems dealing with discretionary access control lists (DACLs) that contain inheritable access control entries (ACEs)
SetSecurityDescriptorDacl	5/16/08 2:39:33 PM	Never use a NULL DACL with an object because any user can change the DACL and owner of the security descriptor.
SetThreadToken	5/16/08 2:39:33 PM	Do not continue execution of a client request if the function fails.
SHCreateDirectory	5/16/08 2:39:33 PM	Vulnerable to TOCTOU issues
SHCreateProcessAsUserW	5/16/08 2:39:34 PM	Use fully qualified executable filename. Do not depend on the shell's heuristics to locate the file.
ShellExecute	5/16/08 2:39:34 PM	Use fully qualified executable filename. Do not depend on the shell's heuristics to locate the file.
SHFileOperation	5/16/08 2:39:34 PM	Vulnerable to TOCTOU issues
SHGetFileInfo	5/16/08 2:39:34 PM	Vulnerable to TOCTOU issues
SHGetFolderPath	5/16/08 2:39:34 PM	The destination string buffer must be long enough to hold the return file path.
-SHGetNewLinkInfo	5/16/08 2:39:34 PM	pszName buffer needs to be at least MAX_PATH in length. Vulnerable to TOCTOU issues.
SHGetPathFromIDList	5/16/08 2:39:34 PM	The destination string buffer must be long enough to hold the return file path.
SHILCreateFromPath	5/16/08 2:39:35 PM	Vulnerable to TOCTOU issues
SHIsFileAvailableOffline	5/16/08 2:39:35 PM	Vulnerable to TOCTOU issues
SHPathPrepareForWrite	5/16/08 2:39:35 PM	Vulnerable to TOCTOU issues

SHRegGetPath	5/16/08 2:39:35 PM	The destination string buffer must be long enough to hold the return file path.
SHValidateUNC	5/16/08 2:39:35 PM	Vulnerable to TOCTOU issues
SIGNAL-01	5/16/08 2:39:35 PM	Avoid using signals or at least keep them short to avoid preemptive interference and reentrancy issues.
SIGNAL-02	5/16/08 2:39:35 PM	Disable signals before executing setuid(root).
SNPRINTF	5/16/08 2:39:35 PM	Be careful with string formatting operations.
Socket	5/16/08 2:39:35 PM	Care must be exercised when a process with elevated permissions grants or allows children processes to inherit its rights.
SPRINTF	5/16/08 2:39:35 PM	Be careful with string formatting operations.
STAT	5/16/08 2:39:36 PM	Vulnerable to TOCTOU issues
Statvfs()	5/16/08 2:39:36 PM	Vulnerable to TOCTOU issues
STLSTRING	5/16/08 2:39:36 PM	Beware of copying non-terminated strings into the STL <string> class.
STRCAT	5/16/08 2:39:36 PM	The strcat() function is unsafe and should not be used.
StrCatBuff	5/16/08 2:39:36 PM	Always ensure buffer is null terminated.
StrCatChainW	5/16/08 2:39:36 PM	The result of StrCatChainW() is not guaranteed to be null terminated.
STRCMP	5/16/08 2:39:36 PM	Will fail if passed unterminated strings
STRCPY	5/16/08 2:39:36 PM	The string copy library functions are vulnerable to buffer overflow attack.
STRECPY	5/16/08 2:39:36 PM	The strecpy() and streadd() functions are dangerous unless care is taken to allocate a large enough output buffer.
StrFormat_	5/16/08 2:39:37 PM	Carefully manage buffer sizes.
StringCch_W	5/16/08 2:39:37 PM	Carefully specify appropriate units.
STRLEN	5/16/08 2:39:37 PM	Beware of use with strings that are not null terminated.

STRNCAT	5/16/08 2:39:37 PM	Requires careful tracking of character count in the buffer and use of appropriate units, and must be null terminated.
STRNCPY	5/16/08 2:39:37 PM	Make sure the buffer and bounds are the proper size to hold the source string plus a NULL character.
STRTRNS	5/16/08 2:39:37 PM	Vulnerable to buffer overflows
Strxfrm, Wcsxfrm	5/16/08 2:39:37 PM	Carefully manage buffer sizing and units. Ensure entire string is transformed.
Symlink	5/16/08 2:39:37 PM	Vulnerable to TOCTOU issues
SYSLOG-1	5/16/08 2:39:38 PM	Always bound input to avoid internal buffer overflow.
SYSLOG-2	5/16/08 2:39:38 PM	syslog() is subject to format string vulnerabilities.
T_Open	5/16/08 2:39:38 PM	Securely specify and protect target filename.
TMPNAM-TMPFILE	5/16/08 2:39:38 PM	Vulnerable to TOCTOU issues
Truncate	5/16/08 2:39:38 PM	Vulnerable to TOCTOU issues
TTYNAME	5/16/08 2:39:38 PM	Can return a non-null-terminated string.
Umask	5/16/08 2:39:38 PM	Carefully restrict permissions for a file upon creation.
UnicodeToBytes	5/16/08 2:39:39 PM	Poses a risk of buffer overflow if the return buffer is not appropriately sized.
Unlink	5/16/08 2:39:39 PM	Vulnerable to TOCTOU issues
Utime	5/16/08 2:39:39 PM	Vulnerable to TOCTOU issues
Utmpname	5/16/08 2:39:39 PM	Vulnerable to TOCTOU issues
VFORK	5/16/08 2:39:39 PM	Vulnerable to race conditions. Don't use vfork() in your programs.
WideCharToMultiByte	5/16/08 2:39:39 PM	The destination string buffer must be long enough to hold the same number of characters, not bytes, as contained in the source string.
WinExec	5/16/08 2:39:39 PM	Vulnerable to white space issues in executable or path name. Applications should use the CreateProcess function.
Wsprintf	5/16/08 2:39:40 PM	Be careful with string formatting operations.